Medianet Media Awareness

Q. What is Medianet Media Awareness?

A. Medianet Media Awareness enables the network to become application context-aware end to end. The network works together with the video endpoints and applications for optimal quality of experience and improved visibility.

Media Awareness is a collection of techniques to detect a wide variety of applications and includes:

- Flow Metadata is a network protocol as well as a feature of both Cisco IOS® Software and the Media Services Interface (MSI) that manages and shares application attributes to network devices, allowing appropriate policies to be applied at each hop, end to end.
- Media Services Proxy (MSP) is a Cisco IOS Software feature that uses lightweight deep-packet-inspection techniques to snoop standards-based signaling protocols. MSP produces flow metadata attributes that can be shared among network nodes.
- Cisco® Network-Based Application Recognition 2 (NBAR2) is a Cisco IOS Software feature that provides protocol and application detection using deep packet inspection from a network device.

Q. Why do I need Media Awareness?

A. As applications and application types proliferate and evolve, there is a need for identifying them to provide differentiated policies. Media Awareness allows administrators to differentiate applications and extract actionable information about the application flows in the network. This information can be applied in several ways:

- Enhance quality-of-service (QoS) policies: Prioritize voice and video and protect business-critical applications.
- Simplify and accelerate troubleshooting by deriving actionable information for e.g. “John from Finance has trouble with WebEx® video” as opposed to just IP addresses and port numbers.

Q. Why do I need different Media Awareness techniques?

A. All three techniques are complementary to one another. Flow metadata is explicit application signaling that is supported by Cisco products that have the Media Services Interface. Flow metadata provides a comprehensive view of the flow end to end as it is supported on both Cisco® routing and switching platforms.

MSP provides a subset of MSI services on behalf of endpoints that do not possess MSI. MSP can glean flow attributes from traditional or third-party endpoints through standard protocols (for example, Session Initiation Protocol [SIP], H.323, Skinny Client Control Protocol [SCCP], Session Description Protocol [SDP], and Real Time Streaming Protocol [RTSP]).

MSP cannot provide information that cannot be gleaned by observation of protocols. For example, if the signaling protocols are encrypted, MSP is severely limited. There is additional application contextual information such as importance of session and ad-hoc vs. scheduled nature of the session that would not be

represented in standard signaling; there is no way for the MSP to surmise these attributes. In such cases, application integration with the MSI would provide the explicit application announcement using metadata.

Similarly, deep-packet-inspection techniques such as NBAR2 are unable to provide the additional application context if the information simply is not visible on the wire—it is locked away within the application. Metadata can enhance application awareness in these situations.

MSP and NBAR2 are complementary techniques in that NBAR2 inspects payloads whereas MSP examines signaling protocols.

It is important to appreciate that metadata is the organization of information about a flow, but metadata is also a network protocol for sharing this information among routers and switches along a path. The metadata network protocol allows not only for the application to share information with the network but also for the network devices to generate information (using deep packet inspection, for example) and share it with both other network devices and endpoints.

Q. Do I have to have Flow Metadata in all my network elements for it to work?

A. No. Medianet features have been designed so that every network element on the path is not required to be medianet-enabled. Flow Metadata originates from the MSI, or generated by MSP from a network node, and is passed on to the other network elements in the path. The network elements that do not have this capability will simply forward the flow metadata to the next element in the path. Those network elements that do not support flow metadata along the path would not (of course) be able to apply smarter policies that use the flow metadata attributes.

Q. What happens if I have third-party network elements in my topology?

A. Flow Metadata attributes can just pass through these elements. Please also see the answer for the above question, “Do I have to have Flow Metadata in all my network elements for it to work?”

Q. If I have third-party endpoints or legacy Cisco endpoints, will Media Awareness work?

A. Yes, because it is the primary function of MSP, which is designed to provide flow metadata-like attributes on sessions and flows that are from third-party or legacy Cisco endpoints. Cisco architectures always support industry standards, and therefore Medianet capabilities such as Media Awareness work with all standards-compliant products.

Q. Which Cisco platforms and software releases are supported?

A. Please refer to the Medianet data sheet for an up-to-date detailed description of platforms and versions supported

Q. Does MSP support all third-party endpoints? Which third-party or legacy Cisco endpoints does Media Services Proxy recognize?

A. MSP supports standard protocols such as SIP, H.323, multicast Domain Name System (mDNS), SDP, and RTSP to perform discovery and information element extraction. If the third-party or legacy endpoint supports these protocols, MSP can identify information such as Dial From, Dial To, codec name, application name, etc.

Please refer to the Medianet data sheet for an up-to-date detailed description of Cisco platforms and versions supported.

Media Services Proxy recognizes third-party endpoints that support standard signaling protocols. Vendors of other applications and endpoints are strongly encouraged to participate in interoperability testing through the Cisco Developer Network in order to be fully supported.

Q. Does MSP support Microsoft Office Communications Server (OCS)?

A. MSP supports all products that comply with standard protocols such as SIP and are visible to the network. All products that meet these two criteria can be supported. In order to be fully supported, vendors are encouraged to participate in the interoperability testing of their products through the Cisco Developer network.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C67-706162-01 06/12